WHAT'S NEW IN GRAYLOG 3.0?

POPULAR VOTE 🖐

Who’s using…

POPULAR VOTE 🖐

Who’s using…

- Elastic Stack (ex-ELK)

POPULAR VOTE 🖐

Who's using...

- Elastic Stack (ex-ELK)
- Splunk

POPULAR VOTE 🖐

Who's using…

- Elastic Stack (ex-ELK)
- Splunk
- Some Logging SaaS (Loggly, Scalyr, etc.)

POPULAR VOTE 🖐

Who's using…

- Elastic Stack (ex-ELK)
- Splunk
- Some Logging SaaS (Loggly, Scalyr, etc.)
- Graylog

WHY CENTRALIZED LOGGING?
THAT IS AN EXCELLENT QUESTION

DEBUGGING

Jan Lehnardt
@janl
Folgen
Debugging in three easy steps:
1. look at the logs.
2. if you don't have logs, add logs.
3. look at the logs.
Original (Englisch) übersetzen
RETWEETS
344
GEFÄLLT
467
DON'T PANIC
14:26 - 10. Okt. 2016

DEBUGGING (2)

Honest Status Page
@honest_update

Folgen

We replaced our monolith with micro services so that every outage could be more like a murder mystery.

Tweet übersetzen

01:10 - 8. Okt. 2015

3.009 Retweets **2.616** „Gefällt mir“-Angaben

21 3,0 Tsd. 2,6 Tsd.

SECURITY (1)

A theme in this article will be: "what separates standard incidents from horrifying nightmares?"

A good or bad story around logging will dictate the rest of the incident.

Learning From A Year of Security Breaches

SECURITY (2)

I recommend that any security or infrastructure team putting off a comprehensive approach to logging drop nearly everything to invest in it.

Learning From A Year of Security Breaches

SECURITY (3)

A10:2017 Insufficient Logging & Monitoring

Exploitation of insufficient logging and monitoring is the bedrock of nearly every major incident.

OWASP Top 10 2017

GRAYLOG

GRAYLOG

- Open source log management platform

GRAYLOG

- Open source log management platform
- Built for security and operations

GRAYLOG

- Open source log management platform
- Built for security and operations
- Easy to set up, powerful features

GRAYLOG

- Open source log management platform
- Built for security and operations
- Easy to set up, powerful features
- Extensible via plugins

GRAYLOG 💸

GRAYLOG 💸

- Commercial plugins (Audit log, Archiving, Reporting, Views)

GRAYLOG 💸

- Commercial plugins (Audit log, Archiving, Reporting, Views)
- Professional support

GRAYLOG 💸

- Commercial plugins (Audit log, Archiving, Reporting, Views)
- Professional support
- Link: Graylog Enterprise

Archives

The Graylog archive feature allows you to create archives from indices. The generated archives are simple flat files that can be moved to cheap storage and re-imported at any time.

Overview Configuration Manage Backends

Archive your old indices automatically by setting your index retention strategy to archive on the indices page.

Create Archive for Index

Select an index to be archived to disk. This action will not close or delete the original index.

graylog_6 (10,532 documents / 8.8MB) Archive index

Configuration

Backend:	File System - /tmp/graylog-archive
Max segment size:	500.0MB
Compression type:	gzip
Checksum type:	CRC32 (little endian)
Restore index batch size:	1,000

Archive Catalog 1 total

Rebuild Catalog Archive documentation

Enter search query... Search Reset Export Results

Show: 20

Index	Created	Range	Content	Streams	Restored
graylog_6	a few seconds ago	Feb 7, 10:15 - 13:46	10,516 msgs (4 hours)	All messages, Apache Logs	

« ‹ 1 › »

Audit Log

Graylog Audit Log lets you create a chronological record of activities performed in Graylog, that you can later use to reconstruct and examine the sequence of events that occurred when investigating an event.

Overview Configuration

You can modify the audit log configuration in the Graylog configuration file. Please remember to restart the server afterwards. Read more in the documentation.

Audit Log Entries 472 total

Enter search query... Search Reset Export Results

Show: 20

Timestamp	Actor	Action	Message
2019-02-07 13:31:36.495	admin	delete	system notification of type "generic" deleted
2019-02-07 13:31:27.062	admin	create	search job for search 5c5c251e225a6896b4f143b2 created
2019-02-07 13:31:26.984	admin	create	search job for search 5c5c251e225a6896b4f143af created
2019-02-07 13:31:26.911	admin	create	search 5c5c251e225a6896b4f143b2 created
2019-02-07 13:31:26.873	admin	create	search 5c5c251e225a6896b4f143af created
2019-02-07 13:31:24.769	admin	create	search job for search 5c5c2516225a6896b4f1439e created
2019-02-07 13:31:21.745	admin	create	search job for search 5c5c2516225a6896b4f1439e created
2019-02-07 13:31:21.507	admin	create	search job for search 5c5c2516225a6896b4f1439e created
2019-02-07 13:31:21.026	admin	create	search job for search 5c5c2516225a6896b4f1439e created
2019-02-07 13:31:18.775	admin	create	search job for search 5c5c2516225a6896b4f1439e created
2019-02-07 13:31:18.747	admin	create	search job for search 5c5c2516225a6896b4f1439e created
2019-02-07 13:31:18.521	admin	create	search 5c5c2516225a6896b4f1439e created
2019-02-07 13:31:13.495	admin	create	search job for search 5c5c2511225a6896b4f14399 created
2019-02-07 13:31:13.329	admin	create	search 5c5c2511225a6896b4f14399 created
2019-02-07 13:29:05.678	admin	create	search job for search 5c5c2491225a6896b4f14394 created
2019-02-07 13:29:05.454	admin	create	search 5c5c2491225a6896b4f14394 created

INPUTS

- GELF
- Beats (Filebeat, Metricbeat, etc.)
- Syslog
- CEF
- Netflow (v5 and v9)

INPUTS (COMMUNITY)

- Redis
- MQTT
- SNMP
- AWS Flow Logs, Cloudwatch Logs, CloudTrail
- Many more on the Graylog Marketplace

graylog Marketplace

Explore | Submit | Sign out

Hundreds of Add-ons for Graylog.

How would you like to extend Graylog today?

Search Marketplace

Browse Add-ons by Type

- Plugin
- Content Pack
- GELF Library
- Other Solutions

graylog Marketplace

Search Marketplace

Explore | Submit | Sign out

‹ Back to listing

Space weather input

free!

Plugin v1.0

Ever needed a proof that a solar storm made a bit flip and your code crash? Now you can! Correlate proton density to the response time of your app and the ion temperature to your exception rate.

space weather fun

lennartkoopmann

Download from Github | View on Github | 0 | 59

Published	Last Push	Marketplace Rating	Discussion
23 Oct 16:11	28 Apr 05:44		3 Comments

Readme from Github

Graylog Spaceweather plugin (Solar data)

(This is not actually providing any value at all - except fun and the possibility to decently nerd out)

graylog

all categories ▸ | Categories | Latest | New (4) | Unread (2) | Top | + New Topic

Category	Topics
Announcements This is where we'll post important Graylog updates, such as new releases, product updates, and other useful information.	1 / month
Installation New to Graylog? We've created this category for discussions on installing your Graylog setup.	41 / month 1 unread
Maintenance Have questions on maintaining Graylog after installation? Post it here.	93 / month 1 unread 4 new
Development This is the place to discuss and ask questions about the development of a Graylog-related project	11 / month
Graylog Add-ons Use this category for all things related to add-ons from the Graylog Marketplace such as installation and usage of plugins, content packs, etc	11 / month

Latest	
Indices routing • new Maintenance	5 1m
Msg from one stream stored not only in configured index set, but also in default one • new Maintenance	0 1h
Could not execute search after new installation 3 Installation	4 1h
Not getting data on Collector-Sidecar • new Maintenance	0 2h
Unable to load user list after upgrade to 2.2.2 1 Maintenance	2 2h
Graylog not processing data • new Maintenance	0 2h
Pipeline: Create new message, set this message with new	

graylog | Search | Streams | Alerts | Dashboards | Sources | System | In 0 / Out 0 msg/s | Help | Jochen Schalanda

Search in the last 1 day | Not updating | Saved searches

Type your search query here and press enter. ("not found" AND http) OR http_response_code:[400 TO 404]

Search result

Found **13,958,769 messages** in 1,342 ms, searched in 8 indices.
Results retrieved at 2017-03-27 16:50:52.

Add count to dashboard | Save search criteria | More actions

Fields | Decorators

Default | All | None | Filter fields

- account_id
- action
- application_name
- aws_source
- bssid
- bytes
- capture_window_duration_seconds
- channel
- dns_op_code
- dns_question
- dns_question_class
- dns_question_type
- dns_response_code

List fields of **current page** or all fields.

Histogram

Add to dashboard

Year, Quarter, Month, Week, Day, Hour, **Minute**

Messages

Previous | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Next

Timestamp	source
2017-03-27 16:50:47.360	EC2AMAZ-57J1961
An account failed to log on. Subject: Security ID: S-1-0-0	
2017-03-27 16:50:46.419	EC2AMAZ-57J1961
An account failed to log on. Subject: Security ID: S-1-0-0	
2017-03-27 16:50:43.068	graylog-defcon
DNS Query: collectd.librato.com	

graylog | Search | Streams | Dashboards | Sources | System | In 0 / Out 0 msg/s | Help | Administrator

FOF/WOF system aggregates

Events below the Drupal layer

Update in background | Fullscreen | Unlock / Edit

Drag widgets to any position you like in unlock / edit mode.

Sec events > warning

in a few seconds

11,745

Message count

in a few seconds

173,429

Failed login attempts

in a few seconds

Value	%	Count
Top values		
teamspeak	5.25%	151
admin	4.10%	118
1pute	3.82%	110
ec----	3.82%	110
amazonaws	3.82%	110
Others		
ec2-54-247-89-36	3.82%	110
eu-west-pute	3.82%	110
pute	3.82%	110
eu-west-1pute	3.82%	110

Chatty applications

in a few seconds

Value	%	Count
Top values		
sshd	28.08%	47,820
CRON	24.61%	41,921
postfix	21.49%	36,601
uptime	10.14%	17,266
pop3d	7.88%	13,421
Others		
imapd	6.42%	10,931
proftpd	1.03%	1,749
ntpd	0.21%	364
pop3d-ssl	0.04%	70
sudo	0.03%	58
su	0.03%	48
dhclient	0.02%	27
imapd-ssl	0.01%	22
rsyslogd	0.01%	15
logger	0.00%	4

Global event rate

in a few seconds

Private cloud 1-minute load average

in a few seconds

AWS 1-minute load average

in a few seconds

Rackspace 1-minute load average

in a few seconds

graylog Search Streams Alerts Dashboards Sources System In 82 / Out 82 msg/s Help Jochen Schalanda

AWS Networks

AWS network FlowLog overview

Update in background | Fullscreen | Unlock / Edit

Drag widgets to any position you like in unlock / edit mode.

Top rejected packet sources

a few seconds ago

Rejected packet sources

a few seconds ago

Value	%	Count
Top values		
172.30.1.147	17.24%	8,496
172.30.2.187	17.01%	8,383
93.174.93.136	0.83%	409
89.163.144.243	0.80%	395
163.172.206.209	0.74%	366
Others		
61.164.149.128	0.44%	217
54.239.39.130	0.39%	191
54.239.39.230	0.37%	184
176.32.118.53	0.33%	164

Global activity

a few seconds ago

Global rejected packets

a few seconds ago

Rejected packet ports

a few seconds ago

Value	%	Count
Top values		
23	14.91%	7,348
0	4.24%	2,087
5358	3.60%	1,775
22	2.89%	1,425
7547	2.37%	1,166
Others		
5060	1.56%	768
3389	1.34%	662
2323	1.24%	610
33434	0.89%	438

graylog Search Streams Alerts Dashboards Sources System In 0 / Out 0 msg/s Help Jochen Schalanda

WiFi IDS

WiFi IDS

Update in background | Fullscreen | Unlock / Edit

Drag widgets to any position you like in unlock / edit mode.

All channels in use

a few seconds ago

Value	%	Count
Top values		
1	34.76%	28,156
11	27.98%	22,664
6	27.92%	22,615
4	4.74%	3,841
9	2.03%	1,646
Others		
3	1.50%	1,219
8	0.39%	316
5	0.32%	257
7	0.18%	146
10	0.17%	138
2	0.00%	3

Networks in reach

a few seconds ago

Value	%	Count
Top values		
SH_Utility 2	16.96%	32,346
SH_Guest	16.85%	32,138
SH_Office	15.90%	30,324
HIDDEN	7.85%	14,984
Wemap	3.77%	7,200
Others		
Free Karma by Women In Tech	3.77%	7,194
\x00\x00\x00\x00\x00\x00\x00\x00	3.50%	6,685
Effort Guest	2.92%	5,567
HTXLabs_Guest	2.64%	5,032

Signal Quality

a few seconds ago

Access Points

a few seconds ago

Value	%	Count
Top values		
E2:55:7D:AE:B5:81	23.74%	7,200
E2:55:7D:AD:F8:21	23.74%	7,200
E2:55:7D:B0:A5:51	23.68%	7,181
02:18:4A:13:8B:11	23.63%	7,166
E2:55:7D:AF:BF:91	4.86%	1,475
Others		
02:18:4A:13:92:C1	0.34%	102

Our Channels

a few seconds ago

Value	%	Count
Top values		
11	38.22%	11,590
6	33.28%	10,091

Encrypted Corporate Netwo...

a few seconds ago

Value	%	Count
Top values		
true	100.00%	30,324

GRAYLOG 3.0

GRAYLOG SIDECAR

💥 GRAYLOG SIDECAR

- Centralized config management for log shippers

💥 GRAYLOG SIDECAR

- Centralized config management for log shippers
- Completely new implementation

💥 GRAYLOG SIDECAR

- Centralized config management for log shippers
- Completely new implementation
- Allows managing arbitrary binaries

💥 GRAYLOG SIDECAR

- Centralized config management for log shippers
- Completely new implementation
- Allows managing arbitrary binaries
- Runs on Linux & Windows

graylog Search Streams Alerts Dashboards Sources Enterprise System / Sidecars In 0 / Out 0 msg/s Help Administrator

Sidecars Overview

The Graylog sidecars can reliably forward contents of log files or Windows EventLog from your servers.

Overview Administration Configuration

Do you need an API token for a sidecar? Create or reuse a token for the *graylog-sidecar* user.

Find sidecars Find Reset Include inactive sidecars

Show: 50

Name	Status	Operating System	Last Seen	Node Id	Sidecar Version	
filebeat	Running	Linux	a few seconds ago	devopsmuc-2019-filebeat	1.0.0	Manage sidecar Show messages
metricbeat	Running	Linux	a few seconds ago	devopsmuc-2019-metricbeat	1.0.0	Manage sidecar Show messages

« ‹ 1 › »

GROK EDITOR

💥 GROK EDITOR

- Grok == Regular Expressions on Steroids

💥 GROK EDITOR

- Grok == Regular Expressions on Steroids
- Sometimes hard to debug

💥 GROK EDITOR

- Grok == Regular Expressions on Steroids
- Sometimes hard to debug
- No more external Grok Debugger

💥 GROK EDITOR

- Grok == Regular Expressions on Steroids
- Sometimes hard to debug
- No more external Grok Debugger
- Grok editor now with preview and test

graylog Search Streams Alerts In 2 / Out 2 msg/s Help Administrator

Grok patterns

This is a list of grok patterns you can use in your Graylog g

Import pattern file | Create pattern

Filter patterns

Name	Pattern	Actions
BASE10NUM	(?<![0-9.+-])(?>[+-]?(?:	Delete Edit
BASE16FLOAT	\b(?<![0-9A-Fa-f.])(?:[+	Delete Edit
BASE16NUM	(?<![0-9A-Fa-f])(?:[+-]?	Delete Edit
CISCOMAC	(?:(?:[A-Fa-f0-9]{4}\.){	Delete Edit
COMBINEDAPACHELOG	%{COMMONAPACHE	Delete Edit
COMBINEDAPACHELOG_FLOG	%{IPORHOST:clientip ... {NUMBER:response;s ... rsion})?|%{DATA:rawrequest})" %	Delete Edit
COMMONAPACHELOG	%{IPORHOST:clientip ... {NUMBER:bytes}|-) ... est})" %{NUMBER:response} (?:%	Delete Edit
COMMONMAC	(?:(?:[A-Fa-f0-9]{2}:){5	Delete Edit
DATA	.*?	Delete Edit
DATE	%{DATE_US}|%{DATI	Delete Edit
DATE_EU	%{MONTHDAY}[./-]%	Delete Edit
DATE_US	%{MONTHNUM}[/-]%	Delete Edit
DATESTAMP	%{DATE}[-]%{TIME}	Delete Edit
DATESTAMP_EVENTLOG	%{YEAR}%{MONTHN	Delete Edit
DATESTAMP_OTHER	%{DAY} %{MONTH} %	Delete Edit
DATESTAMP_RFC2822	%{DAY}, %{MONTHD	Delete Edit

Edit Grok Pattern DATE

Name

DATE

Under this name the pattern will be stored and can be used like: '%{THISNAME}' later on

Pattern

%{DATE_US}|%{DATE_EU}

The pattern which will match the log line e.g: '%{IP:client}' or '.*?'

Filter pattern

BASE10NUM Add
(?<![0-9.+-])(?>[+-]?(?:(?:[0-9]+(?:\.[0-9...

BASE16FLOAT Add
\b(?<![0-9A-Fa-f.])(?:[+-]?(?:0x)?(?:(?:[0...

BASE16NUM Add
(?<![0-9A-Fa-f])(?:[+-]?(?:0x)?(?:[0-9A-F...

Sample Data

7.2.2019

Here you can add sample data to test your pattern

Test with Sample Data

Test Result


```
{
  "DATE": "7.2.2019",
  "DATE_EU": "7.2.2019",
  "MONTHNUM": [
    null,
    "2"
  ],
  "YEAR": [
```


Will contain the result of your test in a JSON format

Cancel Save

💥 CONTENT PACKS 2.0

💥 CONTENT PACKS 2.0

- Sharing configuration between Graylog clusters

💥 CONTENT PACKS 2.0

- Sharing configuration between Graylog clusters
- Allow using parameters

💥 CONTENT PACKS 2.0

- Sharing configuration between Graylog clusters
- Allow using parameters
- Versioning

💥 CONTENT PACKS 2.0

- Sharing configuration between Graylog clusters
- Allow using parameters
- Versioning
- Removal (uninstall)

graylog | Search | Streams | Alerts | Dashboards | Sources | Enterprise | System / Content Packs | In 2 / Out 2 msg/s | Help | Administrator

Content Selection

Parameters

Preview

Previous | Next

Parameters list

Create parameter

Enter search query... | Filter | Reset

Title	Name	Description	Value Type	Default Value	Used	Action
Beats Input Port	BEATS_PORT	Port for the Beats input (default: 5044)	integer	5044	✓	Delete Edit

Entity list

Enter search query... | Filter | Reset

Title	Type	Description	Origin	Used Parameters	Action
					Show
IPV6	grok_pattern			0	Edit Show
IPV4	grok_pattern			0	Edit Show
Beats	input			1	Edit Show
GeoLite2-City	lookup_adapter			0	Edit Show

Details

Version: 1
Name: DevOps Munich
Summary: Content Pack for DevOps Munich Feb 7, 2019
Vendor: Jochen
URL:
ID: `8d469db5-5ccc-4069-b108-e5d713970ec4`
Parameters: 1
Entities: 41

graylog Search Streams Alerts Dashboards Sources Enterprise System / Content Packs In 1 / Out 1 msg/s Help Administrator

Content Selection

Parameters

Preview

Previous Next

Edit

Config Key

Choose Config Key

Parameter

Choose...

Apply

Config Key	Parameter	Action
configuration.port	BEATS_PORT	Clear

Close

1
DevOps Munich Content Pack for DevOps Munich Feb 7, 2019
Jochen

8d469db5-5ccc-4069-b108-e5d713970ec4
1
41

Title	Type	Description	Origin	Used Parameters	Action
					Show
IPV6	grok_pattern			0	Edit Show
IPV4	grok_pattern			0	Edit Show
Beats	input			1	Edit Show
GeoLite2-City	lookup_adapter			0	Edit Show

💥 VIEWS 💸

💥 VIEWS 💸

- Interactive dashboards

💥 VIEWS 💸

- Interactive dashboards
- Completely customizable

💥 VIEWS 💸

- Interactive dashboards
- Completely customizable
- Can be saved and shared

graylog | Search | Streams | Alerts | Dashboards | Sources | Enterprise / Views | System | In **2** / Out **2** msg/s | Help | Administrator

Query#1 ✖ +

View Actions

Search in the last 1 hour

× Apache Logs

*

Apache Logs

Apache Logs

+ Create

Found **712 messages** in 155ms.
Query executed at 2019-02-07 12:33:00.

View Description

Search Details

Fields

Filter fields | Reset

List fields of **current streams**, all or all including reserved fields.

- agent
- auth
- auth_id
- beats_type
- bytes
- city
- clientip
- continent
- coordinates
- country

Message Count

Transfered Bytes per User Agent

agent	sum(bytes)	count()
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_8_4) AppleWebKit/5352 (KHTML, like Gecko) Chrome/40.0.813.0 Mobile Safari/5352	99919	1
Mozilla/5.0 (Windows NT 6.1; en-US; rv:1.9.0.20) Gecko/1986-23-12 Firefox/37.0	99693	1
Mozilla/5.0 (X11; Linux i686) AppleWebKit/5352 (KHTML, like Gecko) Chrom	99537	1

Total data transfer

Distribution error responses

💥 REPORTING 💸

💥 REPORTING 💸

- For your management team 😉

💥 REPORTING 💸

- For your management team 😉
- Create shiny reports (PDF)

💥 REPORTING 💸

- For your management team 😉
- Create shiny reports (PDF)
- Allows scheduling of report creation

💥 REPORTING 💸

- For your management team 😉
- Create shiny reports (PDF)
- Allows scheduling of report creation
- Reports can automatically be sent via email

graylog Search Streams Alerts Dashboards Sources Enterprise / Reports System In 2 / Out 2 msg/s Help Administrator

Scheduling

Choose the recipients for this report and when the report should be scheduled for delivery.

☐ Send this report automatically on a regular basis

Frequency

Select a frequency

Select how often this report should be sent out.

Email subject

Set an email subject to use when sending the report.

Email body

Add an email body to use when sending the report.

User recipients

Type username

Select Graylog usernames that will receive this report.

Email recipients

Type email address

Add email addresses that will receive this report.

Update scheduling Cancel

Layout

This is a preview of the report. Drag and drop widgets to sort the report contents, your changes will be updated automatically.

DevOps Munich 2019

My shiny subtitle

end of cover page

Some description. Yay!

Client Location

WHAT'S IN A GRAYLOG CLUSTER?

WHAT'S IN A GRAYLOG CLUSTER?

- Graylog

WHAT'S IN A GRAYLOG CLUSTER?

- Graylog
- Elasticsearch 5.6 or higher

WHAT'S IN A GRAYLOG CLUSTER?

- Graylog
- Elasticsearch 5.6 or higher
- MongoDB 2.4 or higher

WHAT'S IN A GRAYLOG CLUSTER?

- Graylog
- Elasticsearch 5.6 or higher
- MongoDB 2.4 or higher
- Optional: Graylog Collector Sidecar

Devices and
Applications /
Log Messages
Server
Graylog
MongoDB
Elasticsearch
Browser
(Client)

Devices and Applications / Log Messages
Browser (Client)
HTTP(S)
Syslog
Gelf
Beats
Loadbalancer
Availability Check (API)
HTTP(S)
Syslog
Gelf
Beats
Server
Elasticsearch
Server
Elasticsearch
Server
Elasticsearch
Elasticsearch Cluster
Server
Graylog
MongoDB
Server
Graylog
MongoDB
Server
Graylog
MongoDB
Replica Set

Configuration
Configuration
Rest API
Graylog
INPUTS
Graylog
Sidecar
manages / configures
nxlog /
winlogbeat
Log
messages
Graylog
Sidecar
manages / configures
nxlog /
filebeat
Windows Host
Linux Host

LIVE DEMO 😱

Open Demo

QUESTIONS? 🤔

CONTACT DETAILS

– – in –

ADDITIONAL LINKS

- Graylog
- Graylog Documentation
- Graylog Marketplace
- Graylog Community Forums

IMAGE CREDITS

- "Log Truck" by Oregon Department of Transportation is licensed under CC BY 2.0
- Tony Stark GIF at Giphy
- Wiggeling Cat GIF at Giphy
- Lincoln Stoll (@lstoll)